Commonwealth of Kentucky
Cabinet for Health and Family Services

Cabinet for Health and Family Services (CHFS) Information Technology (IT) Policy

050.101 Privacy and Security Awareness Program Policy

Version 2.4
July 24, 2019

Revision History

Date	Version	Description	Author
11/30/2006	1.0	Effective Date	CHFS OATS Policy Charter Team
6/5/2019	2.3	Review Date	CHFS OATS Policy Charter Team
7/24/2019	2.4	Revision Date	CHFS OATS Policy Charter Team

Sign-Off

Sign-off Level	Date	Name	Signature
Executive Advisor (or delegate)	7/24/2019	Jennifer L. Harp	
CHFS Chief Information Security Officer (or delegate)	7/24/2019	DENNIS E. LEBER	

Table of Contents

1 Policy Definitions

- **Agency:** Defined by CHFS for the purpose of this document, agency or agencies refers to any department within CHFS.
- **Confidential Data:** Defined by the Commonwealth Office of Technology (COT) Standards Data of which the Commonwealth has a legal obligation not to disclose. This data requires the highest levels of restrictions, because of the risk or impact that will result from disclosure, modifications, breach, or destruction of that data. Examples include, but are not limited to, data not releasable under the Kentucky State Law (Kentucky Revised Statute 61.878); Protected Health Information; Federal Tax Information; Social Security and Credit Card numbers
- **Contract Staff/Personnel:** Defined by CHFS as an employee hired through a state approved (i.e. System Design/Development Services {SDS} Vendor Agreement/Company) vendor who has a master agreement with the state.
- **Electronic Protected Health Information (ePHI):** Defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule as individually identifiable health information, including demographic data, that relates to: the individual's past, present or future physical or mental health or condition, the provision of health care to the individual, or the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual. Personally identifiable health information items include many common identifiers (e.g., name, address, birth date, Social Security Number). The Privacy Rule excludes from protected health information employment records that a covered entity maintains in its capacity as an employer and education and certain other records subject to, or defined in, the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g.
- **Federal Tax Information (FTI):** Defined by Internal Revenue Service (IRS) Publication 1075 as federal tax returns and return information (and information derived from it) that is in the agency's possession or control which is covered by the confidentiality protections of the Internal Revenue Code (IRC) and subject to the IRC 6103(p) (4) safeguarding requirements including IRS oversight. FTI is categorized as Sensitive but Unclassified information and may contain personally identifiable information (PII). FTI includes return or return information received directly from the IRS or obtained through an authorized secondary source, such as Social Security Administration (SSA), Federal Office of Child Support Enforcement (OCSE), Bureau of the Fiscal Service (BFS), or Centers for Medicare and Medicaid Services (CMS), or another entity acting on behalf of the IRS pursuant to an IRC 6103(p) (2) (B) Agreement. FTI includes any information created by the recipient that is derived from federal return or return information received from the IRS or obtained through a secondary source.
- **Insider Threat:** Defined by National Institute of Standards and Technology (NIST) 800-53 Revision 4 an entity with authorized access (i.e., within the security domain)

that has the potential to harm an information system or enterprise through destruction, disclosure, modification of data, and/or denial of service.

- **Personally Identifiable Information (PII):** Defined by Kentucky Revised Statute (KRS) Chapter 61 House Bill 5 (HB5) and in accordance with NIST 800-53 Revision 4 as information which can be used to distinguish or trace the identity of an individual; person's first name or first initial and last name, personal mark, or unique biometric or genetic print or image, in combination with one or more of the following data elements: account number, credit card number or debit card number that in combination with any required security code, access code or password would permit access to an account; social security number, taxpayer ID number, driver's license number, state ID number, passport number or other ID number issued by the United States government, or individually identifiable health information, except for education records covered by The Family Educational Rights and Privacy Act of 1974 (FERPA).
- **Security Awareness Training:** Defined by NIST 800-53 Revision 4 as the organizations determine the appropriate content of security awareness training and security awareness techniques based on the specific organizational requirements and the information systems to which personnel have authorized access. The content includes a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents. The content also addresses awareness of the need for operations security.
- **Sensitive Data:** Defined by COT standards as data that is not legally protected but should not be considered public information and only be disclosed under limited circumstances. Only authorized users should be granted access to sensitive data. Examples include: All information identifiable to an individual including staff, employees, and contractors but not limited to dates of birth, driver's license numbers, employee ID numbers, license plate numbers, and compensation information. The Commonwealth proprietary information including but not limited to intellectual property, financial data and more.
- **Sensitive Financial Data (including PCI):** Defined by Payment Card Industry (PCI) Data Security Standards (DSS) Security Standards as cardholder and sensitive authentication data including Primary Account Number (PAN), cardholder name, expiration date, service code, full track data (magnetic stripe data or equivalent on a chip0, Card Security Codes such as CAV2/CVC2/CVV2/CID, and PIN(s). CHFS also defines sensitive financial data as anything that is inclusive of bank identification/information (i.e. bank routing number, account number, etc.).
- **State Staff/Personnel:** Defined by CHFS as an employee hired directly through the state within the CHFS with final approval and appointment by the Kentucky Personnel Cabinet.
- **Third Party**: Defined by CHFS as any contracted or government organization that is not a part of the agency's organizational structure. This may include state or federal auditing agencies, state approved security contract vendors or other external organization whose capabilities can be determined sufficient to conduct assessment needs. An engineering technique used to identify threats, attacks, vulnerabilities and countermeasures that could affect your application.

- **Vendor Staff/Personnel:** Defined by CHFS as an employee contracted through an approved Master Business Associate Agreement, or other formal agreement, to provide temporary work for CHFS.

2 Policy Overview

2.1 Purpose

The Cabinet for Health and Family Services (CHFS) Office of Application and Technology Services (OATS) must establish a comprehensive level of security controls through a privacy and security program. This document establishes the agency's Privacy and Security Awareness Program Policy to manage risks and provide guidelines for security best practices regarding training.

2.2 Scope

The scope of this policy applies to all internal CHFS state, contract, and vendor staff/personnel, temporary personnel, third party providers under contract with a CHFS agency, and other entities that interact with CHFS information related resources. This policy covers the applicable computer hardware, software, application, configuration, business data, and data communication systems. External vendors or other defined groups/organizations providing information security or technology services may work with the CHFS agency(s) to request exceptions to this policy.

2.3 Management Commitment

OATS Division Directors, the CHFS Chief Technical Officer (CTO), Chief Information Security Officer (CISO), and IT Executive Management have reviewed and approved this policy. Senior Management supports the objective put into place by this policy. Violations of not abiding by this policy may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. CHFS shall report illegal activities or theft of CHFS property (physical or intellectual) to the appropriate authorities.

2.4 Coordination among Organizational Entities

OATS coordinates with CHFS organizations and/or agencies that access applications, systems, and facilities. All organizational entities that interact with CHFS are subject to follow requirements outlined within this policy.

2.5 Compliance

As the official guidance domain for this policy, CHFS agencies abide by the security and privacy requirements established in applicable state laws and regulations as well as federal guidelines outlined in the NIST. Additionally, applicable agencies follow security and privacy frameworks outlined within the Centers for Medicare and Medicaid Services (CMS), the Internal Revenue Services (IRS), and the Social Security Administration (SSA).

3 Roles and Responsibilities

3.1 Chief Information Security Officer (CISO)

An individual responsible for providing guidance and direction in assessment, planning, and implementation of all security standards, practices, and commitments required. This individual is responsible for adherence to this policy.

3.2 CHFS OATS Information Security (IS) Team

The CHFS OATS IS team is responsible for the assessment, planning, and implementation of all security standards, practices, and commitments required.

3.3 Chief Privacy Officer (CPO)

An individual responsible for overseeing activities related to the development, implementation, maintenance of, and adherence to the Cabinet's and Commonwealth's information privacy and confidentiality policies and procedures in compliance with federal and state laws. This individual will conduct HIPAA self-assessments through coordination with the Information Security Agency Representative, the CISO, or CHFS OATS IS team, and other CHFS agencies, and will ensure compliance with HIPAA notification and reporting requirements in the event of an identified breach. This position is responsible for adherence to this policy.

3.4 Security/Privacy Lead

Individuals are designated by the division leadership to coordinate privacy and/or security issues and incidents with all appropriate personnel. This individual(s) is responsible for providing privacy and security guidance for protection of PII, ePHI, FTI and other financial sensitive information to all CHFS staff and contractor personnel. This role along with the CHFS OATS IS team is responsible for adherence to this policy.

3.5 CHFS Contract, State, and Vendor Staff/Personnel

All CHFS contract, state, and vendor staff/personnel must adhere to this procedure. All staff/personnel must comply with referenced documents, found in Section 8 Policy References below that pertain to the agency's applications, application servers, appliances, operating systems, web servers, network components, and database (server or components) that reside on CHFS/OATS information system(s).

3.6 CHFS OATS IS Training Administrator

A CHFS OATS IS training administrator or delegate oversees the entire life cycle of the security and privacy awareness training program. This includes annual training initiation, reminders, noncompliant reporting, and escalation to management, as needed.

4 Policy Requirements

4.1 General

This policy defines and details the requirement for privacy and security awareness that data owners are expected to implement to safeguard their computing assets. All new employees and contractors are presented with access to enterprise and cabinet privacy and security policies, standards, procedures, and the CHFS Employee Privacy and Security of Protected Health, Confidentiality, and Sensitive Information Agreement (CHFS 219 or 219V Form), prior to the provision of access to any CHFS computing asset. All CHFS employees and contract staff shall be reminded annually of their privacy and security responsibilities. Additionally, the OATS IS Team and the Commonwealth Office of Technology (COT) Security Management Branch are responsible for sending out periodic reminders concerning contemporaneous privacy and security events as well as current privacy and security risks.

To satisfy the requirement for the Privacy and Security Awareness Program, CHFS OATS IS team in conjunction with CPO will develop, implement, and maintain a training program to foster awareness of policies and procedures related to information privacy and security. Basic privacy and security awareness training to all state and contract staff must be provided as necessary and appropriate to carry out their duties. Employees and staff who have access to PII or PHI will receive the appropriate Privacy training. At a minimum, Security and Privacy training will be provided:

- Prior to system access
- When major system change occurs
- Annually thereafter

All CHFS agencies will complete standardized training provided by the Information Security Department's training administrator through the Kentucky Online Gateway (KOG). To satisfy agency requirements, a multi-question test will be taken at the end of the training session requiring a passing score of no less than 75 percent. Documentation showing completion of training for staff or quiz results must be retained for at least ten (10) years in accordance with the CHFS Records Retention Schedule Kentucky Department for Libraries and Archives (KDLA) requirements.

The training materials will be reviewed annually and updated as needed, or when there is a material change in applicable law or CHFS's privacy and security policies and procedures. CHFS will provide additional training to employees and staff in the event that job functions are affected by such a material change.

4.2 Training Content

The training administrator is responsible for providing the Privacy and Security Awareness Training content to KOG. The training at a minimum shall consist of, but is not limited to the following:

- Security Awareness on recognizing and reporting potential indicators of

compromise or insider threats;
- Incident Response procedures or steps;
- Any federal or state laws and regulations that the agency must follow/abide by;
- Explanation of importance and responsibilities the employee has around identifying and protecting sensitive data;
- Employees' responsibilities related to privacy and security in the workplace.

Additional information for the content and requirements for CHFS annual awareness training can be found in the CHFS Privacy and Security Awareness Training Procedure.

5 Policy Maintenance Responsibility

The OATS IS Team is responsible for the maintenance of this policy.

6 Policy Exceptions

Any exceptions to this policy must follow the guidance established in CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy.

CHFS agencies, such as Child Support Enforcement (CSE), that do not utilize KOG to perform privacy and security awareness training, will be responsible for maintaining documents of proof to ensure privacy and security awareness activities are annually completed.

7 Policy Review Cycle

This policy is reviewed at least annually and revised on an as needed basis.

8 Policy References

- Centers for Medicare and Medicaid Services (CMS) MARS-E 2.0
- CHFS Confidentiality/Security Agreement/Internet and Electronic Policies and Procedures- CHFS-219 Form
- CHFS OATS Form: IRS FTI Safeguard Training Certification Acknowledgement Form
- CHFS OATS Policy: 070.203 Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy
- CHFS OATS Procedure: CHFS Privacy and Security Awareness Training Procedure
- CHFS Office of Human Resources Management (OHRM) Personnel Procedures Handbook, Chapter II: 2.10
- CHFS Records Retention Schedule Kentucky Department for Libraries and Archives (KDLA)

- Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule
- Internal Revenue Services (IRS) Publication 1075
- Kentucky Information Technology Standards (KITS): 4080 Data Classification Standard
- Kentucky Revised Statue (KRS) Chapter 61: House Bill 5 (HB5)
- National institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
- Payment Card industry (PCI) data Security Standard (DSS) Requirements and Security Assessment Procedures Version 3.2.1
- Social Security Administration (SSA) Security Information
- U.S. Department of Education Family Educational Rights and Privacy Act (FERPA)